

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,443	01/13/2001	Francisco Corella	10001558-2	9963

22879 7590 09/02/2004

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/759,443

Applicant(s)

CORELLA, FRANCISCO

Examiner

Michael R Vaughan

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 January 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-59 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-59 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 January 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 14 papers.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claims 1-59 have been examined and are pending.

Specification

Applicant is required to update the status (pending, allowed, etc.) of all parent priority applications in the first line of the specification. The status of all citations of US filed applications in the specification should also be updated where appropriate.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449 is attached to the instant Office action.

Claim Rejections - 35 USC ' 112, second paragraph

Claims 15, 16, 35, and 36 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 15 and 35 do not distinctly claims the subject matter because they contradict their parent claims. Claims 1 and 21

Art Unit: 2131

discloses that the registration authority maintain a certificate database. Claims 15 and 35 refute this limitation by disclosing the registration authority does not maintain a certificate database. Clarification and/or correction are required.

Claim Rejections - 35 USC ' 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8, 10, 14,15, 17-28, 30, 35 are rejected under 35 U.S.C. 102(b) as being anticipated by Ramasubramani (USP 6,233,577).

As per claims 1, 21 Ramasubramani teaches an off-line (landnet, col. 7, line 56) registration authority for issuing unsigned (undesigned) public key validation certificate (col. 7, lines 35-37) that binds a public key of the subject to a first public key serial number (ID) (col. 7, line 48), maintaining a certificate database (col. 7, line 38) which stores the unsigned PKVC, an online credentials server for issuing a disposable public key validation certificate to the subject (col. 7, lines 42-45) from the first unsigned

Art Unit: 2131

PKVC, and maintain a table that contains entries corresponding to valid PKVCs (col. 7, lines 38-39).

As per claims 2, 22 Ramasubramani teaches the PKVN are unique (col. 7, line 1).

As per claims 3, 23 Ramasubramani teaches the subject can invalidate the first unsigned PKVC entry in the table (col. 12, lines 13-15).

As per claims 4, 24 Ramasubramani teaches the registration authority generates a public key revocation code to be used by the subject in its revocation request (col. 12, lines 1-11).

As per claims 5, 25 Ramasubramani teaches a secure channel that provides data (col. 7, lines 55-560).

As per claims 6, 26 Ramasubramani teaches an expiration date/time (col. 2, line 10).

As per claims 7, 27 Ramasubramani teaches a validity period from when the credentials server issues the disposable PKVC to the expiration date/time is sufficiently

Art Unit: 2131

short such that the disposable PKVC does not need to be subject to revocation (col. 2, lines 10).

As per claims 8, 28 Ramasubramani teaches the disposable PKVC is not subject to revocation (col. 12, lines 5-7).

As per claims 10, 30 Ramasubramani teaches a PKVC is issued in response to a message from the subject (col. 7, line 46).

As per claims 14, 34 Ramasubramani teaches the PKVC can be verified for authentication by demonstrating knowledge of a private key (col. 11, lines 42-45).

As per claims 15, 35 Ramasubramani teaches the registration authority maintains a certificate database (col. 7, lines 38).

As per claim 17, Ramasubramani teaches the credentials server ceases to issue PKVC binding to the first PKVN (col. 12, lines 6-8).

As per claim 18, Ramasubramani teaches removing the table entry (col. 12, lines 6-9).

As per claim 19, Ramasubramani teaches marking the first unsigned certificate in the database as being invalid (col. 12, lines 6-9 and lines 20-25).

As per claim 20, Ramasubramani teaches verifying the request for revocation that includes the previously generated PKRC (col. 12, lines 1-25).

Claims 37-47, 49-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Perlman et al, hereinafter Perlman (USP 6,230,266).

As per claim 37, Perlman teaches a subject (col. 2, lines 2), a first public key validation agent maintaining a record of the status of the public key (col. 2, lines 1-10), having a high probability of being unique, and a verifier configured to respond to an authentication of the subject and ascertaining the validity of the subject's public key (col. 2, lines 55-60).

As per claim 38, Perlman teaches binding the subject's public key to a public key validation number (see Fig 5).

As per claim 39, Perlman teaches the PKVN are unique (col. 2, line 3).

As per claim 40, Perlman teaches issuing a first certificate indicating the binding (col. 2, lines 1-9).

As per claim 41, Perlman teaches issuing a second certificate indicating the validity of the subject's public key (col. 6, lines 60-67).

As per claim 42, Perlman teaches the first PKVA is configured to respond to a request for invalidating the subject's public key (col. 2, lines 60-62).

As per claim 43, Perlman teaches requiring a first issued certificate in order to issue a second certificate (col. 6, lines 30-35).

As per claim 44, Perlman teaches the second certificate is a signed certificate (col. 6, line 34).

As per claim 45, Perlman teaches the second certificate is a disposable certificate (col. 6, line 34).

As per claims 46 and 47, Perlman teaches an expiration time and date (col. 2, line 5).

As per claim 49, Perlman teaches responding to a request for invalidating a subject's public key (col. 2, lines 24-26).

As per claim 50, Perlman teaches verifying that the request was submitted by an entity having authorization (col. 4, lines 13-15).

As per claim 51, Perlman teaches requiring a revocation code in order to invalidate a subject's public key (col. 6, lines 30-36).

As per claim 52, Perlman teaches verifying that the revocation code coincides with previously generated PKRC (col. 6, lines 30-36).

As per claim 53, Perlman teaches including altering the maintained record (col. 10, lines 54-59).

As per claim 54, Perlman teaches changing the validity status of the public key (col. 10, lines 57).

As per claim 55, Perlman teaches removing the maintained record (col. 10, lines 60-62).

As per claim 56, Perlman teaches altering accessibility to the maintained record (col. 10, lines 36-40).

As per claim 57, Perlman teaches authenticating the subject by verifying one purported identity attribute (col. 11, lines 1-9).

As per claim 58, Perlman teaches responding to the assertion of the validity of the subject's public key is based on the maintained record (col. 11, lines 1-9).

As per claim 59, Perlman teaches certifying the authenticity of the first PKVN and the identifier (col. 11, lines 1-5).

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention

was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 9, 11-13, 16, 29, 31-33, 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ramasubramani in view of Andrews (USP, 6,324,645).

As per claims 9, 16, 29, and 36 Ramasubramani is silent in disclosing maintaining a hash table that contains hashes of valid unsigned PKVC. Andrews teaches maintaining a hash table that contains hashes of valid unsigned PKVC (col. 9, line 59—col. 10, line 7). Using a hash is a way to maintain the validity of a certificate and would be advantageous to verify that a particular certificate has not been changed. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Andrews within the system of Ramasubramani because it would insure that a certificate has not been altered. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claims 11-13 and 31-33, Ramasubramani is silent in disclosing a collision-resistant hash such as SHA-1 and MD5. Andrews teaches the use of such collision resistant hash function. Examiner supplies the same rationale for the motivation to combine Andrews and Ramasubramani as recited in the rejection of claims 9 and 29.

Claims 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman in view of Andrews (USP, 6,324,645).

As per claim 48, Perlman is silent in disclosing maintaining a hash table that contains hashes of valid unsigned PKVC. Andrews teaches maintaining a hash table that contains hashes of valid unsigned PKVC (col. 9, line 59—col. 10, line 7). Using a hash is a way to maintain the validity of a certificate and would be advantageous to verify that a particular certificate has not been changed. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Andrews within the system of Perlman because it would insure that a certificate has not been altered. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan

Examiner

Art Unit 2131


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100